speaking of a natural order among the directions issuing from a point so many difficulties are to be met that a development of the theory of angle along lines similar to those pursued in discussing segments had best not be attempted any earlier than necessary.

Definition of (proper) triangle: *A (proper) triangle is the geometric figure composed of three segments each of which is less than a semi-line drawn so as to connect in pairs three points.* The parts of the triangle are its three sides, and its three angles which are the angles formed by the directions in which the segments leave the vertices. A segment less than a semi-line may be called a proper segment.

Theorem 10. *If two sides and the angle formed by them in one triangle are congruent to two sides and the angle formed by them in another triangle, the triangles are congruent.*

As two angles are congruent the triangles may be moved so that these angles coincide. The adjacent sides take the same directions and as they are congruent they must coincide throughout. The third sides will therefore lie on the same line and between the same points of the line. Of the two segments which satisfy these conditions one is greater than a semi-line and cannot form the side of a proper triangle. Hence the other segment must be the third side of each triangle and the triangles coincide throughout.

Theorem 11. *If a side and two adjacent angles of one triangle are congruent to a side and two adjacent angles of a second triangle, the triangles are congruent.*

Theorem 9 is needed in the proof—which is left to the reader. A similar proof may be given for the following:

Theorem 12. *If two angles are congruent their vertical angles are also congruent.*

Theorem 13. *If three directions a, b, c radiate from a point and three directions a', b', c' from the same or a different point and if furthermore the congruences $\measuredangle ab \equiv \measuredangle a'b'$ and $\measuredangle ac \equiv \measuredangle a'c'$ are fulfilled, then $\measuredangle bc \equiv \measuredangle b'c'$.*

ON SOME SPECIAL ARITHMETIC CONGRUENCES.

By H. S. VANDIVER, Bala, Pa.

If we take the well known relation

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)\,2} (\mathrm{mod}\, p),$$

where p is a prime, and suppose that $p \equiv 3 (\mathrm{mod} 4)$, then

$$\left(\frac{p-1}{2}!\right)^2 \equiv 1 (\mathrm{mod} p) \ldots\ldots (1),$$

$$\frac{p-1}{2}! \equiv \pm 1 (\mathrm{mod} p) \ldots\ldots (2).$$

The question is, what analytic relations govern this ambiguous residue? Dirichlet (*Werke*, Vol. I, p. 107) called attention to the problem, and Jacobi (*Crelle*, Vol. 9, p. 189) enunciated and proved a theorem connected with it. Kronecker (Liouville, Vol. 3, 2nd series, p. 269) gave another theorem which may be used as a practical rule for determining the sign in any particular case. I wish to discuss here some relations connected with Jacobi's theorem, which is as follows:

If p is a prime number of the form $4n+3$, then

$$\frac{p-1}{2}! \equiv (-1)^{\mu} (\mathrm{mod} p)$$

where μ is the number of quadratic non-residues of p which are less than $\frac{1}{2}p$.

Jacobi's proof of this depends on the theory of quadratic forms. Another proof is easily obtained from the formula

$$\left(\frac{p-1}{2}!\right)^{(p-1)/2} \equiv \frac{p-1}{2}! (\mathrm{mod} p),$$

the truth of which is evident from (2) (see Bachmann, *Niedere Zahlentheorie*, Vol. I, pp. 178-9). The theorem shows that the least residue of $\frac{p-1}{2}! (\mathrm{mod} p)$ is known as soon as the evenness or oddness of μ is determined. There are a number of other questions in the theory of numbers which involve a consideration of this same criterion, and some of them will be investigated here. It is necessary to make use of the analysis in another demonstration of Jacobi's theorem.

Consider the series

$$1^2, 2^2, 3^2, \ldots\ldots, \left(\frac{p-1}{2}\right)^2 \ldots\ldots (3),$$

and calculate the residues of these numbers, modulo p, between the limits $\frac{1}{2}(p-1)$ and $-\frac{1}{2}(p-1)$. No two of these residues can be equal in absolute value. For, let α^2 and β^2 be two terms of (3) which give equal remainders, irrespective of sign. Then

$$\alpha^2 \equiv \pm \beta^2 (\mathrm{mod} p).$$

Now we cannot have $\alpha^2 - \beta^2 \equiv 0 (\mathrm{mod} p)$ since neither $\alpha - \beta$ nor $\alpha + \beta$ is zero, and each is less than p. The relation $\alpha^2 + \beta^2 \equiv 0 (\mathrm{mod} p)$ is also impossible since p has the form 3(mod4). Hence the absolute values of the residues are identical, in some order, with the integers

$$1, 2, 3, \ldots\ldots, \tfrac{1}{2}(p-1).$$

The positive residues in question constitute all the quadratic residues of p which are less than $\frac{1}{2}p$. Consequently there will be precisely as many negative residues as there are quadratic non-residues less than $\frac{1}{2}p$. By multiplication we then obtain

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^\mu \left(\frac{p-1}{2}!\right) (\mathrm{mod}\, p),$$

from which the theorem follows, $\frac{p-1}{2}!$ being prime to p. This proof is of some interest in itself, since no use is made of Wilson's theorem.

Let $-\alpha_1, -\alpha_2, \ldots, -\alpha_\mu$, be the negative least residues, modulo p, for the numbers in the series (3), and $\beta_1, \beta_2, \ldots, \beta_k$, the positive residues. Now write

$$1^2 = [1^2/p]p + r_1, \quad 2^2 = [2^2/p]p + r_2, \ldots, (p')^2 = [(p')^2/p]p + r_{p'},$$

where $[m/n]$ represents the largest integer in m/n, and $p' = \frac{1}{2}(p-1)$. Hence $r_1, r_2, \ldots, r_{p'}$ are the least *positive* residues for the series (3), modulo p. They are therefore identical apart from their order with $p-\alpha_1, p-\alpha_2, \ldots, p-\alpha_\mu$, $\beta_1, \beta_2, \ldots, \beta_k$. Hence by addition,

$$1^2 + 2^2 + 3^2 + \ldots + (p')^2 = Mp + \mu p + B - A,$$

$$\text{or } \tfrac{1}{24}p(p-1)(p+1) = Mp + \mu p + B - A \ldots (4),$$

where

$$M = [1^2/p] + [2^2/p] + \ldots [(p')^2/p], \quad A = \alpha_1 + \alpha_2 + \ldots + \alpha_\mu, \quad B = \beta_1 + \beta_2 + \ldots + \beta_k.$$

Since $\alpha_1, \alpha_2, \ldots, \alpha_\mu, \beta_1, \beta_2, \ldots, \beta_k$, are the numbers $1, 2, \ldots, p'$ in a certain order,

$$A = \tfrac{1}{8}(p^2-1) - B.$$

Upon substitution in (4), the resulting relation may be written

$$\mu p + M \equiv \tfrac{1}{24}p(p^2-1) + \tfrac{1}{8}(p^2-1) (\mathrm{mod}2).$$
$$\therefore \mu \equiv M + \tfrac{1}{24}(p+3)(p^2-1) (\mathrm{mod}2).$$

Now for $p = 4n+3$, $\frac{1}{24}(p+3)(p^2-1) = \frac{1}{8}(2n+3)(n+1)(4n+2) \equiv 0 (\mathrm{mod}2)$. Hence the interesting conclusion, $\mu \equiv M (\mathrm{mod}2)$. The number M may be expressed by means of circular functions on applying the relation

$$\left[\frac{m}{n}\right] = \frac{m}{n} - \tfrac{1}{2} + \frac{1}{2n} \sum_{k=1}^{n-1} \sin \frac{2km\pi}{n} \cot \frac{k\pi}{n},$$

where m and n are positive integers, n not a factor of m (Eisenstein, *Crelle*, XXVII, p. 281).

The residue of μ modulo 2 occurs in the investigation of the following question: If a is any primitive root of the prime $p=4n+3$, then the least absolute residues of a, a^2, ..., $a^{\frac{1}{2}(p-1)}$, modulo p, are the integers 1, 2, 3, ..., $\frac{1}{2}(p-1)$, in some order. For no two of them can be equal in absolute value or we would have a congruence of the form

$$a^\alpha \equiv \pm a^\beta , \quad a^{\alpha-\beta} \equiv \pm 1 (\mathrm{mod} p) \qquad [\beta < \alpha < \tfrac{1}{2}(p-1)]$$

which is impossible since $\alpha-\beta$ is less than $\frac{1}{2}(p-1)$. The residues are then distinct, and we get by multiplication, ν being the number of residues in question which are negative,

$$a^{\frac{1}{8}(p^2-1)} \equiv (-1)^\nu \frac{p-1}{2}! \ (\mathrm{mod} p).$$

But $a^{\frac{1}{8}(p^2-1)} \equiv (-1)^{n+1}$, $\frac{1}{2}(p-1)! \equiv (-1)^\mu (\mathrm{mod} p)$. $\therefore \nu = \mu + n + 1 \ (\mathrm{mod} 2)$.

We might ask whether there is not a method for determining $\mu (\mathrm{mod} 2)$, based on a theory of distribution of quadratic residues. But there appears to be but one general fact known regarding the residues less than $\frac{1}{2}p$, namely,

If p is a prime of the form $3 (\mathrm{mod} 4)$, *then in the series* 1, 2, 3, ..., $\frac{1}{2}(p-1)$, *there are more quadratic residues of p than non-residues.*

It may be mentioned here that no elementary proof of this theorem has as yet been given.*

If in the first congruence of the paper we put $p=4m+1$, then

$$\left(\frac{p-1}{2}!\right)^2 \equiv -1 (\mathrm{mod} p).$$

Since we can now set $p=a^2+b^2$, we may write

$$\frac{p-1}{2}! \equiv \pm i \ (\mathrm{mod} \overline{a+bi}), \quad i^2 = -1.$$

The theorems concerning this two-valued unit residue are analogous to those which have been developed for the case $p=4n+3$.

For example, make $p=8k+5$, and calculate the least positive residues of (3), modulo p. If m is one of these residues then $p-m$ is also. For, if α^2 is the term of the series corresponding to m, then there is one and only one positive integer β, less than $\frac{1}{2}(p-1)$, such that

$$\beta^2 \equiv p - \alpha^2 (\mathrm{mod} p),$$

as follows from the fact that p has the form $1 (\mathrm{mod} 4)$ (Bachmann, l. c., p. 195).

*For what appears to be the only proof known, and which is not elementary, see Smith, *Works*, Vol. I, p. 275, 3rd foot-note.

Hence the residues may be put into two classes, $2k+1$ of them less than $4k+2$, and $2k+1$ of them greater than $4k+2$. Represent these by $r_1, r_3, \ldots, r_{2k+1}$, and $s_1, s_2, \ldots, s_{2k+1}$, respectively. Now find a positive integer N_γ such that

$$S_\gamma \equiv \pm iN_\gamma \pmod{a+bi}$$

where γ is arbitrary and $N_\gamma < \frac{1}{2}(p-1)$. As this involves the solution of a linear congruence in the domain $R(i)$ the unique determination of N_γ is always possible. Hence the residues of (3) can be expressed by

$$r_1, r_3, \ldots, r_{2k-1}, iN_1, iN_2, \ldots, iN_{2k+1} \ldots (5),$$

if we disregard order and sign. Now there cannot be a relation

$$r_\delta \equiv N_\epsilon \pmod{a+bi}.$$

For if f^2 and g^2 are two terms of the series (3) such that $f^2 \equiv r_\delta$, $g^2 \equiv \pm iN_\epsilon \pmod{a+bi}$, then

$$f^2 \equiv \pm ig^2, f^4 + g^4 \equiv 0 \pmod{a+bi}.$$

$\therefore f^4 + g^4 \equiv 0 \pmod{p}$. But this last relation is impossible since p has the form $5 \pmod 8$. Also it is obvious that we cannot have such relations as $r_n \equiv r_\nu$, $N_n \equiv N_\nu \pmod{a+bi}$, where $n = 1, 2, \ldots, 2k+1$, $\nu = 1, 2, \ldots, 2k+1$. Hence the series (5) is identical with $1, 2, \ldots, 4k+2$, in some order. Multiplication then gives, using (3) and (5),

$$[(4k+2)!]^2 \equiv (-1)^{\mu_1} i^{2k+1} (4k+2)! \pmod{a+bi}.$$

Dividing by $(4k+2)!$ which is prime to $a+bi$, and reducing,

$$(4k+2)! \equiv (-1)^{\mu_1+1} i \pmod{a+bi},$$

where μ_1 is the number of negative terms in (5) which are obtained when the N's are given their proper signs.

EXAMPLE. Let $p=13$. Then the numerically least residues of

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2,$$

are $1, 4, -4, 3, -1, -3$. But $-4 \equiv 6i$, $-3 = -2i$, $-1 \equiv -5i \pmod{2+3i}$. $\therefore 6! \equiv -i \equiv 5 \pmod{2+3i}$, $6! \equiv 5 \pmod{13}$.

To develop theorems corresponding to the above for the determination of the least residue of $\left(\frac{q-1}{2}\right)! \pmod q$, where q is a prime of the form $1 \pmod 8$, it would be necessary to make use of complex moduli defined by higher cyclotomic equations. But the treatment of the case $p \equiv 5 \pmod 8$ is sufficient to show the

character of the analysis one would encounter. It is curious that the ambiguities already discussed have an analogue in the following theorem:*

If P is a prime of the form $4c+1$, and $m^2+n^2=P$ (m and n integers), then either m or n has the form $\pm 1 (\mathrm{mod} 4)$. If $m \equiv \pm 1 (\mathrm{mod} 4)$, then

$$m \equiv \pm \frac{(2c)!}{2(c!)^2} (\mathrm{mod} P).$$

Now since $(2c)! \equiv -1 (\mathrm{mod} P)$, we can write

$$(c!)^2 \equiv \pm \frac{1}{2m} (\mathrm{mod} P) \ldots\ldots (7).$$

Hence the least residue of $(c!)^4 (\mathrm{mod} P)$ can be determined uniquely. But in (7) the residue for $(c!)^2 (\mathrm{mod} P)$ is two-valued, and we face a problem which is analogous to Dirichlet's.

ON THE EVALUATION OF CERTAIN DEFINITE INTEGRALS.

By PROFESSOR G. B. M. ZERR, A. M., Ph. D., Philadelphia, Pa.

1. In works on Calculus we find the following:

$$\int_0^\infty e^{-[x^2+(c^2/x^2)]} dx = \tfrac{1}{2}\sqrt{\pi}\, e^{-2c}.$$

We wish to find the value of

$$\int_0^\infty e^{-[fx^2+(g/x^2)]} \sin[hx^2+(k/x^2)] dx = A,$$

$$\int_0^\infty e^{-[fx^2+(g/x^2)]} \cos[hx^2+(k/x^2)] dx = B,$$

as well as of the still more general definite integral C of §6.

In view of the substitution $y = x\sqrt{m}$, we have

$$\int_0^\infty e^{-[mx^2+(n/x^2)]} dx = \frac{1}{\sqrt{m}} \int_0^\infty e^{-[y^2+(mn/y^2)]} dy = \frac{\sqrt{\pi}}{2\sqrt{m}} e^{-2\sqrt{(mn)}}.$$

Now $A = \frac{1}{2\sqrt{-1}} \int_0^\infty \{e^{-(f-h\sqrt{-1})x^2-(g-k\sqrt{-1})(1/x^2)} - e^{-(f+h\sqrt{-1})x^2-(g+k\sqrt{-1})(1/x^2)}\} dx.$

*This theorem is due to Gauss; see Smith, l. c., p. 268.